AN RFID PRIMER AND INTELLECTUAL FREEDOM CATUTION

by J. Douglas Archer

RFID (Radio Frequency Identification) is here. RFID commonly refers to both a system of identifying unique individual items via radio signals and to the tags that are attached to or embedded in those items. Whether pronounced as "are-fids" or spelled out as "R-F-I-Ds," the system and its tags are appearing throughout society – including Indiana libraries. The Mooresville and Speedway Public Libraries are just two examples of recent installations.

THE RFID PRIMER

A generic RFID system consists of a tag, a reader, a connection, and a storage device (computer and database) although in some cases (remote car keys for example) a tag and reader may be sufficient. The tag is attached to an item. The reader sends out a radio signal to the tag that responds with a signal containing data stored on the tag. The connection from the reader to the computer allows the storage of this data for later use. The "How Things Work" website provides a more detailed, well-illustrated explanation of RFID (Bonsor).

Just what are these RFID tags? Some people have referred to them as electronic barcodes. In a non-technical sense that's correct. If so, they are barcodes that speak – and speak with a unique voice. By moving from stripes on a label that must be read and interpreted by a light sensitive scanner to an electronic tag scanned by a radio transmitter/receiver, the information contained on the label/tag in or on an individual item can now be read from a distance without being "seen."

In addition, most barcodes used in commerce are product specific but not item specific. That is, a given traditional barcode might identify a can of soup as a can of Campbell's tomato soup but not indicate the specific can, produced in a specific batch, in a specific plant, on a specific day. RFID tags may be as general or as specific as desired.

Libraries are among the few institutions that are already using item specific barcodes. A library barcode may say this is the library's third copy of Dan Brown's *The Da Vinci Code, a Novel* published by Doubleday in 2003. Therefore, in theory, libraries are a near perfect target market for RFID.

The greatest barrier to common adoption of this technology in libraries and elsewhere has been the unit price of the tags. As prices for tags have come down, their use has expanded enormously. And, of course, as their use has expanded, the unit price has continued to decline (Ward, 2004). Both Wal-Mart and the United States Defense Department are moving toward requiring item specific tags (Tech Trends, 2006). Consequently, RFIDs are now within the budgetary reach of many businesses and government agencies including local libraries.

RFID tags can be dumb or smart. Smart tags are like the computer chips in watches or any other handheld device. They contain their own power source and can broadcast the information contained on them. These systems, often contained in bracelets or collars, have been in use for many years to track livestock, pets, or wild animals. Think *Animal Kingdom*, *Marty Stouffer's Wild Kingdom*, or *Animal Planet*. They have been the bane and blessing of science fiction and adventure movie heroes for decades (e.g., Arnold Schwarzenegger in *Total Recall* and Sean Connery in *Goldfinger*). Now that their size has reached that of a couple of grains of rice, they can be found throughout society. Their most familiar use is in tollway speed passes and remote control car keys.

Dumb RFID tags are sort of like floppy discs. They contain no internal power source and just sit there until stimulated and read by another device. These tags have also gradually decreased in size from notecard or file folder label dimensions to dots that are almost as small as the period at the end of this sentence. Though often embedded in a credit card sized plastic substrate for convenience, they can be painted onto paper stickers much smaller than many commonly used security labels. This is often the form they take in library applications.

Libraries are primarily concerned with dumb rather than smart tags. They have become relatively cheap and serve library purposes well since libraries don't care

where books wander while charged out. They are only concerned that they return and be accounted for at the appropriate time.

Just to make things a bit more complicated both dumb and smart RFID tags come in two varieties, read only and read/write. In this way they are roughly similar to magnetic and optical media such as floppy discs, CDs, and DVDs.

After a little reflection, the benefits of RFID technology for libraries become readily apparent. Since, unlike a barcode, tags do not have to been seen to be read, a book does not have to be opened to be checked out or checked in. In addition it does not need to be removed from the shelf to be inventoried. In fact, most systems now allow multiple items to be read at the same time, eliminating the need to examine items individually. Whether charged out by a staff member or charged out with a self-check machine, repetitive motion injuries are greatly reduced and a great deal of time is saved. Staff can be assigned to more creative duties than opening, scanning, stamping, and closing covers, and patrons can be on their way more quickly. Inventories can actually be run as often as needed or desired.

THE INTELLECTUAL FREEDOM CAUTION

A major potential problem with the implementation of RFID technology in libraries is increased potential access by unauthorized persons to patron data. Since the library profession has come to view patron privacy and confidentiality as key factors in promoting intellectual freedom, the American Library Association's (ALA) Intellectual Freedom Committee (IFC) has prepared a set of guidelines addressing these concerns (American Library Association, 2006). Included in their document is a series of "best practices" that will allow libraries to enjoy the full benefits of this new technology while protecting patron privacy. (These guidelines have been reprinted as an addendum to this article with the permission of ALA's Office for Intellectual Freedom (OIF) and may be accessed from ALA's website at <http://www.ALA.org> by following the path: Home > Our Association > Offices > Intellectual Freedom > Intellectual Freedom Issues > RFID > RFID in Libraries: Privacy and Confidentiality Guidelines.)

The privacy concerns specific to RFIDs addressed in the ALA IFC's guidelines generally fall into four categories, 1) the actual data contained on tags, 2) the transmission of that data from the reader to the library's data management system, 3) the security of RFID generated data, and 4) patron perceptions of library privacy policies and practices.

Data on Tags: In theory, any data on a tag could be read by an unauthorized reader. While present technology requires close proximity for dumb tags, one never knows what advances will be made or when. So, while at the moment a snoop would have to get very close to one's book bag to begin developing a "hotlist" of one's reading habits, who knows how long it will be until he or she will only need to sit in a car in the library's parking lot to be able to scan one's latest acquisitions? Only one thing is certain. If "they" can snoop, "they" will. This has been incontrovertibly demonstrated by numerous recent revelations of government surveillance and data gathering programs. Therefore, libraries would be well advised to place as little personally identifiable information (PII) on tags as possible. In theory, the only information that must be included on a library RFID tag is data identifying the item itself. For maximum security that data should only consist of a code linked to a record in the library's data management system. The code itself should be encrypted. If a library succumbs to temptation and adds additional information to the tag, then encryption becomes even more crucial.

Transmission of Data: At present there are two means of transmitting data from RFID tag readers to the library's data management system, wired and wireless. If a library chooses to use a hardwired connection, then its security concerns are no greater than with any other hardwired connection in its system. Short of a physical tap on the line, the data is relatively secure. However, wireless transmissions can be intercepted. Therefore, if the library chooses to use a wireless method, it should be particularly careful with regard to what data is recorded on tags and how that data is encoded.

Data Storage: RFID presents no major, new security concerns for libraries' data management systems other than accentuating the need for well developed privacy and confidentiality policies and procedures. These include the regular de-linking of PII from item records as soon as the need for the links no longer exists, regular purging of old files, clear delineation of the authority for access to and release of PII, and a thorough understanding of what library data is stored by third parties on non-library systems (e.g., system vendors, database suppliers, and cooperative agencies).

Patron Perceptions: Since many patrons have become more sensitive to the security of their PII over the last two decades (especially since 9/11), it is particularly important for libraries to inform their patrons of the details of any planned RFID installation including privacy safeguards as early in the process as possible. Offering an "opt in" alternative can go a long way to assuage patron concerns.

ALA OIF's guidelines were prepared with these and many other concerns in mind. They do not attempt to prescribe specific technological solutions. Rather, they identify issues and offer advice that may be adapted as new technologies become available.

FURTHER INFORMATION

Finally, the reader should know that some organizations find RFID to be a greater threat to privacy than is reflected in this article. *Consumer Reports* recently addressed data security issues for the general consumer in a feature article ("End of Privacy," 2006). The Electronic Frontiers Foundation has been an opposition leader in the online community (Electronic Freedom Foundation). And, the Library Users Association, a Berkeley, California, based group organized in opposition to the implementation of RFID in the Berkeley Public Library, has challenged any use of RFID in libraries (Warfield & Tien, 2005).

For more information regarding the American Library Association's position on RFID the reader may wish to contact the American Library Association's Office for Intellectual Freedom and, in particular, Deborah Caldwell-Stone, its Deputy Director at dstone@ala.org or 800-545-2433, ext. 4224. Ms. Caldwell-Stone's presentation at the 2005 Indiana Library Federation Annual Conference, while not cited specifically, provided the original impetus for this article.

REFERENCES

American Library Association. Intellectual Freedom Committee. (2006). RFID in libraries: Privacy and confidentiality guidelines. Retrieved August 27, 2006, from http://www.ala.orgTemplate.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=130851

Bonsor, K. How RFIDs work. *How stuff works*. Retrieved August 27, 2006, from http://electronics.howstuffworks.com/smart-label.htm

Electronic Frontiers Foundation. Radio Frequency Identification (RFID). Retrieved August 27, 2006, from http://www.eff.org/Privacy/Surveillance/RFID/

The end of privacy? (2006, June). *Consumer Reports*, *71(6),* 33-39.

Tech Trends (2006, August 22). RFID: The many changes it will bring. *Newsfactor Magazine Online*. Retrieved August 27, 2006, from http://www.newsfactor.com/news/RFID—The-Many-Changes-It-Will-Bring/

Ward, D. (2004, August 26). 5-Cent tag unlikely in 4 years. *RFID Journal*. Retrieved August 27, 2006, from http://www.rfidjournal.com/article/articleview/1098/1/1/

Warfield, P. & Tien, L. (2005, March 4). RFID should be canceled immediately. *Berkeley Daily Planet*. Retrieved August 27, 2006, from http://www.berkeleydailyplanet.com/article.cfm?archiveDate=03-04-05&storyID=20871

ABOUT THE AUTHOR

Doug Archer is Reference and Peace Studies Librarian at the University Libraries of Notre Dame and may be contacted at 109 Hesburgh Library, University of Notre Dame, IN 46556 (archer.1@nd.edu). Doug is an incoming member of ALA's Intellectual Freedom Committee, a continuing member of ILF's Intellectual Freedom Committee, and Vice Chair/Chair Elect of ALA's Intellectual Freedom Round Table.

ADDENDUM

RFID in Libraries: Privacy and Confidentiality Guidelines, adopted by the ALA Intellectual Freedom Committee, June 27, 2006.

Radio Frequency Identification (RFID) technology collects, uses, stores, and broadcasts data. Components of RFID systems include tags, tag readers, computer hardware (such as servers and security gates) and RFID-specific software (such as RFID system administration programs, inventory software, etc.).

RFID technology can enable efficient and ergonomic inventory, security, and circulation operations in libraries. Like other technologies that enable self-checkout of library materials, RFID can enhance individual privacy by allowing users to checkout materials without relying on library staff.

Because RFID tags may be read by unauthorized individuals using tag readers, there are concerns that the improper implementation of RFID technology will compromise users' privacy in the library.[1] Researchers have identified serious general concerns about the privacy implications of RFID use, and particular privacy concerns about RFID use in libraries.[2] Libraries implementing RFID should use and configure the technology to maintain the privacy of library users.

The Council of the American Library Association adopted the "Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles" (Appendix A) and requested the development of guidelines for the implementation of RFID technology in libraries.

Basic Privacy & Confidentiality Principles

Protecting user privacy and confidentiality has long been an integral part of the intellectual freedom mission of libraries.[3] The right to free inquiry as assured by the First Amendment depends upon the ability to read and access information free from scrutiny by the government or other third parties. In their provision of services to library users, librarians have an ethical obligation, expressed in the ALA Code of Ethics,[4] to preserve users' right to privacy and to prevent any unauthorized use of personally identifiable information. As always, librarians should follow these principles when adopting any new technology.

Policy Guidelines

When selecting and implementing RFID technology, librarians should:

- ❒ Use the RFID selection and procurement process as an opportunity to educate library users about RFID technology and its current and future use in the library and society as a whole. A transparent selection process allows a library to publicize its reasons for wanting to implement an RFID system while listening to its users and giving them a larger voice in the public debate over RFID technology.
- ❒ Consider selecting an "opt-in" system that allows library users who wish to use or carry an RFID-enabled borrower card do so while allowing others to choose an alternative method to borrow materials. Because all members who share integrated library systems may not wish to implement an RFID system, this option also may be necessary for library consortia.
- ❒ Review and update appropriate privacy policies and procedures to continue protecting users' privacy, in accordance with Article III of the ALA Code of Ethics and Privacy: An Interpretation of the Library Bill of Rights.[5]
- ❒ Ensure that institutional privacy policies and practices addressing notice, access, use, disclosure, retention, enforcement, security, and disposal of records are reflected in the configuration of the RFID system. As with any new application of technology, librarians should ensure that RFID policies and procedures explain and clarify how RFID affects users' privacy. The ALA Guidelines for Developing a Library Privacy Policy[6] can assist libraries in drafting appropriate policies.
- ❒ Delete personally identifiable information (PII) collected by RFID systems, just as libraries take reasonable steps to remove PII from aggregated, summary data.
- ❒ Notify the public about the library's use of RFID technology. Disclose any changes in the library's privacy policies that result from the adoption of an RFID system. Notices can be posted inside the library and in the library's print and online publications.
- ❒ Assure that all library staff continue to receive training on privacy issues, especially regarding those issues that arise due to the implementation and use of RFID technology.
- ❒ Be prepared to answer users' questions about the impact of RFID technology on their privacy. Either staff at all levels should be trained to address users' concerns, or one person should be designated to address them.

Best Practices

As with any new application of technology, librarians should strive to develop best practices to protect user privacy and confidentiality. With respect to RFID technology, librarians should:

- ❒ Continue their longstanding commitment to securing bibliographic and patron databases from unauthorized access and use.
- ❒ Use the most secure connection possible for all communications with the Integrated Library Systems (ILS) to prevent unauthorized monitoring and access to personally identifiable information.
- ❒ Protect the data on RFID tags by the most secure means available, including encryption.
- ❒ Limit the bibliographic information stored on a tag to a unique identifier for the item (e.g., barcode number, record number, etc.). Use the security bit on the tag if it is applicable to your implementation.
- ❒ Block the public from searching the catalog by whatever unique identifier is used on RFID tags to avoid linking a specific item to information about its content.
- ❒ Train staff not to release information about an item's unique identifier in response to blind or casual inquiries.
- ❒ Store no personally identifiable information on any RFID tag. Limit the information stored on RFID-enabled borrower cards to a unique identifier.
- ❒ Label all RFID tag readers clearly so users know they are in use.
- ❒ Keep informed about changes in RFID technology, and review policies and procedures in light of new information.

Talking to Vendors about RFID

When dealing with vendors, librarians should:

- ❒ Assure that vendor agreements guarantee library control of all data and records and stipulate how the system will secure all information.

- ❒ Investigate closely vendors' assurances of library users' privacy.
- ❒ Evaluate vendor agreements in relationship with all library privacy policies and local, state, and federal laws.
- ❒ Influence the development of RFID technology by issuing Requests for Proposals requiring the use of security technology that preserves privacy and prevents monitoring.

The Request For Information developed by the San Francisco Public Library provides a helpful list of sample questions (Appendix B) to ask when talking to vendors about privacy and their RFID products.

[1]Lori Bowen Ayre, "Wireless Tracking in the Library: Benefits, Threats, and Responsibilities," RFID: Applications, Security, and Privacy, Garfinkle and Rosenberg, eds. (Addison-Wesley, 2006)

[2]David Molnar and David Wagner, Privacy and Security in Library RFID: Issues, Practices, and Architectures, CCS'04, October 25-29, 2004 Washington, D.C.

[3]http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/introduction/introduction.htm

[4]http://www.ala.org/oif/policies/codeofethics

[5]http://www.ala.org/oif/policies/interpretations/privacy

[6]http://www.ala.org/oif/iftoolkits/privacy/guidelines

APPENDIX A: RESOLUTION ON RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY AND PRIVACY PRINCIPLES

WHEREAS, Radio Frequency Identification (RFID) is a technology that uses various electronic devices, such as microchip tags, tag readers, computer servers, and software, to automate library transactions; and

WHEREAS, the use of RFID technology promises to improve library operations by increasing the efficiency of library transactions, reducing workplace injuries, and improving services to library users; and

WHEREAS, many libraries are adopting or in the process of adopting RFID technology to automate library circulation, inventory management, and security control; and

WHEREAS, consumers, consumer groups, librarians, and library users have raised concerns about the misuse of RFID technology to collect information on library users' reading habits and other activities without their consent or knowledge; and

WHEREAS, protecting user privacy and confidentiality has long been an integral part of the mission of libraries; and

WHEREAS, the ALA Code of Ethics states, "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted"; and

WHEREAS, Privacy: An Interpretation of the Library Bill of Rights states that "The American Library Association affirms that rights of privacy are necessary for intellectual freedom and are fundamental to the ethics and practice of librarianship," and calls upon librarians "to maintain an environment respectful and protective of the privacy of all users"; and

WHEREAS, the ALA Intellectual Freedom Committee recognizes the importance of developing policies and guidelines for appropriate implementation of RFID technology in light of the profession's commitment to preserving user privacy and its concern for preserving the trust of library users; and

WHEREAS, the ALA Intellectual Freedom Committee and the ALA Office for Information Technology Policy, recognizing the immediate need to draft privacy principles to protect and promote ALA's values, joined with the Book Industry Study Group (BISG) to form a working group dedicated to developing a set of privacy principles to govern the use of RFID technology by all organizations and industries related to the creation, publication, distribution, and retail sale of books and their use in libraries; now, therefore, let it be

RESOLVED, that the American Library Association endorse the "BISG Policy Statement Policy #002: RFID - Radio Frequency Identification Privacy Principles" (PDF) developed by the IFC and the OITP with the BISG and other working groups; and be it further

RESOLVED, that ALA affirm established privacy norms within and across the business, government, educational, and nonprofit spectrum, specifically acknowledging two essential privacy norms:

Data transferred among trading partners related to customer and/or patron transactions shall be used solely for related business practices and no unauthorized transaction shall be permitted.

Data related to customer and/or patron transactions shall not compromise standard confidentiality agreements among trading partners or information users; and be it further

RESOLVED, that the ALA adopt the following "RFID Privacy Principles" developed by the IFC and OITP with the BISG RFID working group:

All businesses, organizations, libraries, educational institutions and non-profits that buy, sell, loan, or otherwise make available books and other content to the public utilizing RFID technologies shall:

Implement and enforce an up-to-date organizational privacy policy that gives notice and full disclosure as to the use, terms of use, and any change in the terms of use for data collected via new technologies and processes, including RFID.

Ensure that no personal information is recorded on RFID tags which, however, may contain a variety of transactional data.

Protect data by reasonable security safeguards against interpretation by any unauthorized third party.

Comply with relevant federal, state , and local laws as well as industry best practices and policies.

Ensure that the four principles outlined above must be verifiable by an independent audit; and be it further

RESOLVED, that the ALA continue to monitor and to address concerns about the potential misuse of RFID technology to collect information on library users' reading habits and other activities without their consent or knowledge; and be it further

RESOLVED, that the ALA develop implementation guidelines for the use of RFID technologies in libraries.

Adopted by the ALA Council
January 19, 2005
Boston, Massachusetts

APPENDIX B: SECURITY AND PRIVACY SAMPLE QUESTIONS

1. Does the RFID tag have a portion of memory that can be locked (for item number) and a portion that can be re-programmed?
2. What encryption methodologies are available for your RFID tags?
3. Does the RFID tag have or not have a pre-programmed number that would be rendered redundant by unique library item number?
4. Do your RFID tags contain a manufacturer burned in static ID number that cannot be changed by the library, such as for use in a collision-avoidance protocol?
5. Do your tags have a completely silent mode? Can they be "reawakened" from that mode?
6. What information can still be read in the "silent mode" Is there a static identifier built into the chips, such as manufacturer or customer number?
7. Are there access controls, like passwords or keys, which prevent unauthorized readers from reading the tags? If so, do authorized readers first authenticate themselves to the tags, or do tags reveal their IDs first?
8. If passwords or keys protect the RFID tags from unauthorized reading, are the same passwords or keys used by all of your systems, so that one library's readers can read another library's tags? Or are passwords or keys different for each of your systems?
9. If the system uses passwords or keys, how does a reader know which password or key to use? Do readers contain all passwords or keys?
10. Describe the encryption algorithm used with your system in a wireless environment.
11. Who can write to the tags?
12. How can tags be locked so that unauthorized parties cannot write to them?
13. Can the Security Bit be locked by an unauthorized party so that the library cannot unlock it again?
14. Do your tags support the option of writing a random ID to the tag on every checkout, with the library database retaining a map of the random ID to the item's number?
15. How do you address privacy concerns? Please detail.

Permission was granted to publish this section from the Radio Frequency Identification and the San Francisco Public Library Summary Report, prepared by the San Francisco Public Library Technology and Privacy Advisory Committee, October 2005.

To see the entire Summary Report, please visit:

http://sfpl.lib.ca.us/librarylocations/libtechcomm/RFID-and-SFPL-summary-reportoct2005.pdf